UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

DISH NETWORK L.L.C. and NAGRASTAR LLC,	)	
Plaintiffs,	)	
v.	)	Case No. 4:19-cv-03125-AGF
JAMES LEWIS,	)	
Defendant.	)	

MEMORANDUM AND ORDER

This matter is before the Court on the motion of Plaintiffs DISH Network L.L.C. ("DISH") and NagraStar LLC (collectively, "Plaintiffs") for default judgment against Defendant James Lewis. For the reasons set forth below, the motion will be granted in part.

BACKGROUND

In their complaint, filed on November 21, 2019, Plaintiffs allege Defendant trafficked in passcodes used to circumvent Plaintiffs' security system and intercept DISH's encrypted satellite broadcasts of copyrighted television programming. In particular, Plaintiffs contend that they received the records of a confidential informant that oversaw and managed the sale of subscriptions to a pirate television service called NFusion Private Server ("NFPS"). Each subscription consisted of a passcode that enabled access to the NFPS servers. The NFPS servers were used to transmit Plaintiffs' proprietary control words or "keys" over the Internet to the subscriber's receiver pursuant

to a form of piracy known as "Internet key Case sharing" or "IKS" that allowed subscribers to receive DISH's encrypted satellite broadcasts of television programming without authorization. Each IKS Server Passcode was valid for one year. According to Plaintiffs, the records provided by the confidential informant establish that Defendant purchased at least 53 passcodes to the NFPS service, far more than he would need for personal use. Plaintiffs contend that this large-scale purchase demonstrates that Defendant was likely re-selling passcodes to his own customers. Plaintiffs maintain that these IKS Server Passcodes were designed for and have no purpose or use other than to circumvent Plaintiffs' security system and receive DISH programming without purchasing a legitimate subscription from DISH.

Plaintiffs filed suit on November 21, 2019, asserting the following claims against Defendant: "Trafficking In Circumvention Technology And Services In Violation Of The Digital Millennium Copyright Act ['DMCA'], 17 U.S.C. § 1201(a)(2)" (Count I); "Distributing Signal Theft Devices And Equipment In Violation Of The Federal Communications Act ['FCA'], 47 U.S.C. § 605(e)(4)" (Count II); "Circumventing An Access Control Measure In Violation Of The [DMCA], 17 U.S.C. § 1201(a)(1)" (Count III); "Receiving Satellite Signals Without Authorization in Violation of the [FCA], 47 U.S.C. § 605(a)" (Count IV); and "Intercepting Satellite Signals in Violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1)(a) and 2520" (Count V). In their prayer for relief, Plaintiffs sought the greater of actual or statutory damages, permanent injunctive relief, punitive damages, and attorneys' fees and costs.

Plaintiffs filed the return of proof of service on December 2, 2019, indicating that

Plaintiffs served Defendant on November 25, 2019. The process server's sworn "Affidavit of Return of Service" indicates that he served a copy of the summons and complaint on Defendant at Defendant's address of record "by personal service on [Defendant's wife], by reading to, and leaving copy before her, upon her refusal to accept and/or confirm defendant's status at [that address]," and that "St. Louis County Personal Property and Real Estate Records suggest [D]efendant is joint owner as [homeowner] with [his wife] . . . ."[1] ECF No. 5.

Defendant has not filed an answer or other responsive pleading. On Plaintiffs' motion, the Clerk of Court entered default against Defendant on January 22, 2020. ECF No. 12. On January 17, 2020, Plaintiffs filed the instant motion for default judgment as to Counts I and II only, seeking a permanent injunction and statutory damages under the FCA, 47 U.S.C. §§ 605(e)(3)(C)(i)(II), in the amount of $530,000; or, alternatively, statutory damages under DMCA, 17 U.S.C. § 1203(c)(3)(A), in the amount of $132,500. Plaintiffs do not seek actual damages, punitive damages, or attorneys' fees, and they propose that all claims except Counts I and II be dismissed. *See* ECF No. 10-1. Plaintiffs base their motion on the allegations in the complaint, as well as affidavits and

[1] The Court concludes that the process server's affidavit constitutes sufficient proof of proper service under Federal Rule of Civil Procedure 4(e)(2)(B). *See* Fed. R. Civ. P. 4(e)(2)(B) (permitting service by "leaving a copy of [the summons and complaint] at the individual's dwelling or usual place of abode with someone of suitable age and discretion who resides there"); *see also Flores v. Envtl. Tr. Sols., Inc.*, No. PWG-15-3063, 2018 WL 2237127, at *5 (D. Md. May 16, 2018) ("[A]lthough Mr. Johnson 'refused to accept' the copies of the documents in Bestman-Johnson's name, they were left with him[, and] [b]ecause he was at the home he shared with Mrs. Bestman-Johnson, his wife, this qualified as proper service of the summons and complaint on Mrs. Bestman-Johnson under [Rule 4(e)(2)].").

documentation as to liability and damages attached as evidence in support of the motion.

DISCUSSION

"Upon default, the factual allegations of a complaint (except those relating to the amount of damages) are taken as true, but it remains for the court to consider whether the unchallenged facts constitute a legitimate cause of action, since a party in default does not admit mere conclusions of law." *Murray v. Lene*, 595 F.3d 868, 871 (8th Cir. 2010) (citation omitted). Here, the allegations set forth in the complaint, taken as true, along with the evidence attached to Plaintiffs' motion for default judgment, establish that Defendant is liable under Counts I and II of Plaintiffs' complaint.

DMCA, 17 U.S.C. § 1201(a)(2) (Count I)

The DMCA, 17 U.S.C. § 1201(a)(2), states:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that--
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

17 U.S.C. § 1201(a)(2).

Numerous federal courts have recognized that similar allegations of bulk purchasing of IKS Server Passcodes, which have no commercially significant purpose

except to circumvent security systems, "fall squarely within section 1201(a)(2)." *E.g.*, *Dish Network L.L.C. v. Ramirez*, No. 15-CV-04712-BLF, 2016 WL 3092184, at *3 (N.D. Cal. June 2, 2016). The Court likewise finds that Plaintiffs' allegations, taken as true, establish that Defendant violated § 1201(a)(2).

FCA, 47 U.S.C. § 605(e)(4) (Count II)

The FCA, 47 U.S.C. § 605(e)(4), in relevant part, makes it unlawful for any person to sell or distribute any device or equipment while "knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of . . . direct-to-home satellite services . . . ." 47 U.S.C. § 605(e)(4). Accepting Plaintiffs' allegations as true, they establish that Defendant violated § 605(e)(4). *See, e.g.*, *DISH Network L.L.C. v. Simmons*, No. 4:17-CV-53, 2018 WL 3647169, at *5 (E.D. Tenn. June 28, 2018) ("Based on the volume of purchased IKS Server Passcodes, Simmons willfully violated the FCA because he knew or should have known that the codes were unlawful."), *report and recommendation adopted*, No. 4:17-CV-53, 2018 WL 3623764 (E.D. Tenn. July 30, 2018).

Statutory Damages

Although both the DMCA and FCA provide for statutory damages, statutory damages under the relevant provision of the FCA are significantly higher than those under the DMCA and range from $10,000 to $100,000 per violation, as compared to the DMCA's range of $200 to $2,500 per violation. *Compare* 47 U.S.C. § 605(e)(3)(C)(i)(II), *with* 17 U.S.C. § 1203(c)(3)(A). Plaintiffs do not seek—and the Court would not permit—recovery under both statutes because the conduct underlying

the two claims is the same and recovery under both would be duplicative.

Applying the FCA's minimum penalty of $10,000 multiplied by 53 violations, as Plaintiffs seek, would yield a statutory damages award of $530,000. Plaintiffs provide evidence that their injuries "include[] a loss of programming revenues that would ordinarily be received from legitimate subscribers, which are approximately $84 per month on average." ECF No. 11-6 at 5. Considering that each IKS Server Passcode was valid for one year, the annual loss to Plaintiffs occasioned by consumers' use of the 53 pirated IKS Server Passcodes would add up to approximately $53,424. Although the Court recognizes that Plaintiffs' damages may exceed programming revenue losses and, indeed, extend beyond money damages as discussed below, the Court still believes that a statutory damages award of $530,000 is a disproportionate penalty.

Moreover, the facts alleged here fit more squarely under the DMCA. Other courts have so found. *See Dish Network L.L.C. v. Whitehead*, No. 3:09-CV-532-J-32JRK, 2011 WL 6181732, at *6 (M.D. Fla. Dec. 13, 2011). Therefore, the Court believes that Plaintiffs' alternative request for an award of statutory damages under the DMCA in the maximum amount of $2,500 per violation is more appropriate here. *See Simmons*, 2018 WL 3647169, at *6-7 (finding the same).

When determining the amount of damages for each violation under the DMCA, courts consider the willfulness of the conduct as well as the need for deterrence. *Id.* at *7. Considering these factors, and in light of the volume of IKS Server Passcodes purchased by Defendant, Plaintiffs' contention that discovery would have likely uncovered even more violations, and Defendant's failure to appear or defend himself in

this lawsuit, the Court concludes that an award at the high end of the DMCA's range— in the amount of $2,500 per violation—is warranted. *See, e.g., id.* (concluding the same). Multiplying $2,500 by the 53 violations alleged here yields a statutory damages award of $132,500, which the Court finds to be appropriate.

Permanent Injunction

To obtain a permanent injunction, Plaintiffs must demonstrate "(1) that [they have] suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff[s] and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction." *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006).

The Court concludes, particularly in light of Defendant's failure to respond, that Plaintiffs have demonstrated a likelihood of success on the merits of its claims; that Defendant's piracy has irreparably harmed Plaintiffs and will continue to irreparably harm Plaintiffs including by undermining their significant investment in security technology, and by damaging their business reputation and contractual and prospective relationships with programming providers and customers; that the harm to Plaintiffs from Defendant's misconduct outweighs any potential harm to Defendant from enjoining Defendant's piracy; and that the public interest in the enforcement of these federal statutes will be served by an injunction. *See, e.g.*, *Ramirez*, 2016 WL 3092184, at *6-7 (granting permanent injunction based on similar evidence). Therefore, Plaintiffs have established their right to a permanent injunction.

CONCLUSION

Upon review of the record, including Plaintiffs' proposed injunction and order,

IT IS HEREBY ORDERED that Plaintiffs' motion for entry of default judgment is **GRANTED in part** as set forth above. ECF No. 10.

IT IS FURTHER ORDERED that Plaintiffs are entitled to recover statutory damages in the sum of $132,500., and a Permanent Injunction is entered in this case as follows:

Defendant is immediately and permanently **ENJOINED** from:

a. manufacturing, importing, offering to the public, providing, or otherwise trafficking in IKS Server Passcodes, any other code or password used in accessing an IKS server, and any other technology or part thereof that is used in circumventing Plaintiffs' security system or receiving DISH programming without authorization;

b. circumventing or assisting others in circumventing Plaintiffs' security system, or receiving or assisting others in receiving DISH's satellite signal without authorization; and

c. testing, analyzing, reverse engineering, manipulating, or extracting code, data, or information from Plaintiffs' satellite receivers, smart cards, satellite stream, or any other part or component of Plaintiffs' security system.

The Court retains jurisdiction over this action for one year for the purpose of enforcing this final judgment and permanent injunction

IT IS FURTHER ORDERED that the Clerk of Court shall serve a copy of this Order on Defendant at the address reflected in the file.

A separate judgment of default shall accompany this Memorandum and Order.

Audrey G. Fleissig

AUDREY G. FLEISSIG
UNITED STATES DISTRICT JUDGE

Dated this 14th day of April, 2020.